AFRL-RI-RS-TR-2013-139

SECURITY ENGINEERING AND EDUCATIONAL INITIATIVES FOR CRITICAL INFORMATION INFRASTRUCTURES

THE UNIVERSITY OF TULSA

JUNE 2013

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2013-139 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /

ANNA WEEKS
Work Unit Manager

/ S /

ROBERT KAMINSKI
Deputy Chief, Information Exploitation and Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JUNE 2013	FINAL TECHNICAL REPORT	AUG 2009 – Dec 2012

4. TITLE AND SUBTITLE

SECURITY ENGINEERING AND EDUCATIONAL INITIATIVES FOR CRITICAL INFORMATION INFRASTRUCTURES

5a. CONTRACT NUMBER
FA8750-09-1-0208

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
61101E

6. AUTHOR(S)

John Hale, Maurico Papa and David Greer

5d. PROJECT NUMBER
TLSA

5e. TASK NUMBER
09

5f. WORK UNIT NUMBER
22

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The University of Tulsa
800 S. Tucker Drive
Tulsa, OK 74104

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2013-139

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This document is the final summary report of the Security Engineering and Educational Initiatives for critical Information Infrastructures research grant project. The report provides project descriptions fo the 3 major research tasks, highlights specific project accomplishments, identifies project deliverables and lists the 40 publications that were generated over the 3 years of the grant.

15. SUBJECT TERMS
Cyber Physical Systems, Security Engineering, Critical Infrastructure Protection, Human Computer Interaction, Cyber Security Training.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**ANNA WEEKS**
U	U	U	SAR	44	19b. TELEPONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

1.0 SUMMARY 1
2.0 INTRODUCTION 3
2.1 Security Engineering and Testing 3
2.2 Critical Infrastructure Protection Laboratory (CIPL) 5
2.3 Cyber Security Training Center 6
3.0 METHODS, ASSUMPTIONS AND PROCEDURES 8
3.1 Security Engineering – Task 1 8
3.1.1 Technical Rationale and Assumptions. 8
3.1.2 Methods and Procedures. 10
3.2 Critical Infrastructure Protection – Task 2 12
3.2.1 Technical Rationale and Assumptions. 12
3.2.2 Methods and Procedures. 13
3.3 Cyber Security Training – Task 3 18
3.3.1 Technical Rationale and Assumptions. 19
3.3.2 Methods and Procedures. 21
4.0 RESULTS AND DISCUSSION 22
4.1 Security Engineering – Task 1 22
4.2 Critical Infrastructure Protection – Task 2 23
4.3 Cyber Security Training – Task 3 25
5.0 CONCLUSION 27
6.0 REFERENCES 30
APPPENDIX A 33
LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS 38

LIST OF FIGURES

Figure		Page
1	Compound exposure analysis	9
2	Fundamental components of process control systems	14
3	Scaled-down electric power substation	15
4	Control room center	16
5	Distributed monitoring system	17
6	Collaborative STEM education multi-touch devices	25
7	Human Computer Interaction Laboratory	26

1.0 SUMMARY

This three-pronged effort addresses the primary challenges to securing our national cyber space. Complementary initiatives in security engineering, critical infrastructure protection and cyber security training will focus research on technologies, tools and training to protect our most vital information systems and applications. This summary describes the respective contributions from each field and how they will be integrated to derive the maximum benefit from each.

This report is broken out by the three tasks identified in the project: Security Engineering (Task 1), Critical Infrastructure Protection (Task 2), and Cyber Security Training (Task 3).

Security Engineering – Task 1

The activities in the Security Engineering task focused on the development of new technologies enhancing the security engineering process. These activities were broken into three categories; metrics, analytical tools and curriculum development.

- Security Metrics: Development of a primitive, composable collection of metrics to support security engineering development and certification processes.

- System Security Analysis, Testing and Validation: Application of new security metrics and system formalisms to facilitate hardware and software security validation and testing.

- Curriculum Development and Enrichment: Educational content and instructional materials development for computer science, engineering and business undergraduate and graduate curricula to enhance core classes and to define new specialty offerings in the field of security engineering.

Critical Infrastructure Protection – Task 2

The Critical Infrastructure Protection (CIP) Laboratory initiative focused on conducting multidisciplinary research (computer science and electrical engineering) to provide security solutions for the electric power sector and developing smart components to support undergoing efforts to develop a smart grid. Researchers designed and implemented components for securing Process Control System (PCS) networks that have minimal impact on real-time electric power generation and transmission operations while adhering to standards, regulations and best practices. These goals were accomplished by concentrating efforts in the following four major activities:

- Laboratory: A research lab was designed and built to be a close reflection of the most typical components of the power grid to include components that cover power generation, transmission and a control room center.

- Smart Sensor Initiative**:** Researchers leveraged their experience in providing cyber security solutions to the oil & gas industry to develop smart sensors that deliver power more efficiently by providing them with advanced logic components and communication facilities.

- Cyber security in PCS networks**:** Communications between all components must be protected against cyber attacks. This initiative analyzed the communication protocols used by smart sensors to ensure that confidentiality, integrity and availability requirements are satisfied. In the case of legacy systems, protocols were analyzed for vulnerabilities and solutions developed to mitigate risks and strengthen the security posture.

- Access Control and Authentication**:** Securing a highly distributed smart grid requires effective solutions for access control and authentication. Solving the issue of key distribution and revocation in an environment where computational power and communication bandwidth is limited demands the exploration and development of new and adaptation of existing Public Key Infrastructure (PKI) solutions.

Cyber Security Training – Task 3

The Cyber Security Training Center complements the security engineering and critical infrastructure protection initiatives with a strategic blend of curriculum design, development and conversion. This effort focused on next generation online training technologies and techniques to deliver timely, effective and relevant training across multiple audiences.

- Curriculum Design, Development and Conversion: The scope of this task included developing new continuing education courses in digital forensics, critical infrastructure protection and enterprise security based on the Institute for Information Security (iSec) curriculum.

- Content Delivery Methodologies: This part of the effort involved the delivery of instructor led workshops developed from existing iSec curriculum. Concomitant with this task was the identification, construction and customization of a Distance Learning System utilizing next generation e-learning solutions.

- Online Learning Research and Development: The Cyber Security Training Center pursued the development of novel online learning technologies and instructional design techniques that allowed for the effective and efficient delivery of timely and relevant training anywhere in the world. This effort centered on the application of novel Human Computer Interaction (HCI) technologies to virtual learning environments and the development of new metrics that assessed the effectiveness of cyber security training programs and the technology used to identify and deliver content.

While each effort offers its own individual and distinct contributions to the field of information assurance, they supported and validated each other through targeted programmatic initiatives. These programmatic initiatives leveraged critical infrastructure information systems as an attractive application domain for the security engineering research efforts and exploited the technologies innovated from the cyber security training research to support security engineering education and instructional content development and delivery.

2.0 INTRODUCTION

This section presents the introduction and statement of work for three complementary information security initiatives in; (i) security engineering, (ii) critical infrastructure protection, and (iii) cyber security training.

2.1 Security Engineering and Testing

The top 20 software vulnerabilities reported by SANS Institute are populated by the same basic flaws and weaknesses that have plagued the software industry for decades. At the heart of this dilemma is a chronic and alarming gap in the appreciation, mastery and application of security engineering principles [1] and techniques by system designers, administrators and managers.

Lack of security engineering training, tools and metrics is another major obstacle for developers, managers and executives. Software developers must be given practical software assurance tools and trained to use them within a standard framework. Decision-makers must be capable of translating information security intelligence into the lexicon of business. Building a culture of software assurance begins in universities by weaving security engineering principles and processes into mainstream Information Technology (IT) and Information Assurance (IA) computer science, engineering and business curricula.

This project has addressed these challenges with a strategic blend of initiatives aimed at creating new security engineering tools and techniques for practitioners seamlessly integrated into established methodologies. An educational component brings these tools and methodologies into the classroom, exposing undergraduate and graduate students to the motivation and art of security design and testing.

<u>Security Metrics</u>

The scope of this task includes the development of a primitive, but composable collection of metrics to support security engineering development and certification processes. This effort targeted quantitative measures for system vulnerability, based on foundational work in compound exposure analysis [2, 3, 4]. It explored the role of source code analysis tools [5, 6, 7, 8, 9] and correlated the results of compound exposure analysis into abstract threats impacting the operational characteristics of an enterprise.

The core activities in fulfilling this task include:

- Development of primitive metrics with discrete and quantitative properties.
- Construction of composite metrics driven by compound exposure analysis.
- Metric validation via comparative analysis and empirical study.

System Security Analysis, Validation and Testing

iSec researchers investigated methods for system security validation and testing that span software, firmware and hardware boundaries. A mathematical foundation for modeling hybrid system behavior across cyber physical boundaries and capturing relevant security properties was developed. Corresponding analytical tools and techniques based on compound exposure analysis were developed. Strategies for effectively integrating these tools and techniques into a practical security engineering methodology have been pursued and embodied in a software framework.

The targeted results for this research effort thus include:

- Definition of a formal framework for system security analysis, testing and validation.
- Analytical tool prototype for system security specification analysis.
- Integration of tools in a comprehensive security engineering management framework.

Curriculum Development and Enrichment

The development of a model security engineering curriculum is a central element of this project. Weaving security engineering principles and concepts into core computer science and engineering classes will influence the development processes and practices of those responsible for the next generation of information systems and applications. Inserting focused content into information assurance classes, and deploying a class concentrated on the topic of security engineering, affords future security professionals the opportunity to build a specialized skillset in the discipline. The targeted results for this portion of the task accordingly include:

- Instructional modules and laboratories for (i) secure programming and (ii) security engineering within core Computer Science (CS) and engineering courses.
- Course outline, instructional content, labs and exercises for Information System Security Engineering and related IA courses.

2.2 Critical Infrastructure Protection Laboratory (CIPL)

This initiative concentrated its efforts in establishing a state-of-the-art multipurpose Critical Infrastructure Protection Laboratory (CIPL) against cyber attacks in an academic setting. In 1998, Presidential Decision Directive 63 (PDD63) directly emphasized (for the first time) the issue of critical infrastructure protection and recognized that any solutions should address both physical and cyber security. In 2003, Homeland Security Presidential Directive (HSPD) 7 [10] identified 17 sectors that require actions to prepare for, protect against and mitigate the effects of possible attacks or malicious incidents. HSPD7 classifies the energy sector as including electric power and the oil & gas industry. In addition to all the issues associated with cyber security in critical infrastructure protection, the recent rise in energy costs and the strategic importance of energy independence, has highlighted the importance of developing effective ways to deliver electric power to consumers. Studies ordered by the Department o*f* Energy have shown that making the power grid more efficient could save between 46 and 117 billion dollars over the next 20 years [11]. The term used to describe a more efficient power grid is “smart grid.” The smart grid relies on digital technology to improve reliability, reduce cost and save energy. In fact, making our power grid 5% more efficient also helps eliminate the equivalent of greenhouse gas emissions from 53 million cars.

Ongoing development of a “smart grid” will result in the addition of new communicating devices. In addition to the challenges associated with delivering energy efficiently, the introduction of new smart devices will also pose significant research challenges to address cyber security problems.

It is important to note that the Process Control Systems (PCS) community has created standards that adapt information technology security solutions to mitigate risk in industrial control environments. The Instrumentation Systems and Automation’s (ISA) ISA-SP99 Committee on Manufacturing and Control Systems Security has produced two technical reports [12,13] and is currently developing an ANSI/ISA standard. The American Petroleum Institute has released a pipeline Supervisory Control and Data Acquisition (SCADA) security standard API-1164 [14], and the American Gas Association (AGA) has proposed the AGA-12 [15, 16] standard for cryptographic protection of SCADA communications. The United Kingdom’s National Infrastructure Security Co-ordination Centre (NISCC) has released a good practice guide on firewall deployment for SCADA systems and process control networks [17]. Meanwhile, National Institute for Standards and Technology (NIST) has produced two documents, a system protection profile for industrial control systems [18] and a guide for securing control systems [19]. The Department of Energy (DOE) developed a roadmap [20] to secure control systems in the energy sector. The document recognizes the need to produce effective metrics that can be used to measure and assess security postures, to develop and integrate protective measures, to detect intrusions and implement response strategies and the ability to sustain security improvements. The roadmap also describes near term (0-2 years), mid term (2-5) and long term (5-100) milestones and the desired end state for the energy sector for 2015.

In order to maximize the impact of this research thrust, CIPL centered its focus on the energy sector, and more specifically, on the electric power sector. Solutions developed by CIPL adhere to existing standards, regulations and best practices and enable stakeholders to achieve the goals defined by DOE for the electric power sector. In particular, CIPL has addressed these challenges by completing the following tasks:

- Facilities: A research laboratory was designed to be a close reflection of the most typical components of the power grid (for power distribution and consumption). The lab has three major components: (i) a scaled-down electric substation (ring topology) using redundant Programmable Logic Controllers (PLCs), (ii) a state-of-the-art control room center to monitor and visualize the power grid and (iii) a HAN (Home Area Network) facility that looks at the interaction between wireless home automation networks and smart meters used by utilities.

- Smart Sensors: Researchers also leveraged their experience in providing cyber security solutions to the oil & gas industry and developed smart sensors using the Distributed Network Protocol (DNP3) protocol to help deliver power more efficiently.

- Cyber security Solutions: Communications between all components developed by this initiative are also protected against cyber attacks. This achieved by analyzing the communication protocols used by smart sensors to make sure that confidentiality, integrity and availability requirements are satisfied. In the case of legacy systems (Modbus and DNP3), protocols were analyzed for vulnerabilities and solutions developed to mitigate existing risks and strengthen the security posture.

- Access Control and Authentication: Securing a highly distributed smart grid will eventually require effective solutions for access control and authentication. This initiative also tested solutions dealing with access, authentication and key management.

2.3 Cyber Security Training Center

As technology becomes integrated into every aspect of the public and private sectors, the security of critical cyber assets is of paramount importance. Federal, state and local agencies, regulatory bodies and business organizations have all seen recent rules and regulations put in place that govern the levels of security compliance an entity must achieve. A key component of meeting these requirements is the training of the human resources within each organization in practical and current methodologies to ensure the security of these critical assets. A major challenge to both the public and private sectors is designing and implementing an effective cyber security training program that not only aligns with standards and regulations but also provides relevant training across all of their departments and employees. This project addressed these challenges with a strategic blend of cyber security curriculum design, development and conversion with targeted research initiatives aimed at creating next generation distance training technologies and techniques that will deliver timely, effective and relevant cyber security training across multiple audiences.

Curriculum Design, Development and Conversion

The scope of this task included using the latest instructional design techniques to identify and create cyber security training curriculum that map directly to industry and federal standards and certifications. This training curriculum was used to create security awareness programs and is centered on iSec's core research areas of digital forensics, critical infrastructure protection and enterprise security.

New curriculum design and development methodologies were developed to deliver short, focused training curriculum in interactive modules that are categorized by specific topics. This design methodology encouraged regular, even daily training sessions that can be integrated into a student or employee's normal work flow process and help facilitate the comprehension, retention and application of training materials.

In addition, the exploration of role-based training techniques took the concept of training modules to the next level by mapping individual topics not only to standards, regulations and certifications but also to the job roles and requirements of an employee. These techniques were evaluated on how to streamline and target specific training to both public and private sector employees.

The core activities in fulfilling this task included:

- Development of new continuing education courses based off of existing iSec curriculum.
- Use of new instructional design methodologies to create modules of training content.
- Exploring role-based training technique to map modules of content to standards, certifications and job requirements.

Content Delivery Methodologies

The Cyber Security Training Center used a variety of content delivery methodologies beginning with instructor led workshops and evolving into a robust distance training environment. With the identification and conversion of appropriate security content into effective distance learning formats and the application of new content delivery technologies, the Cyber Security Training Center was able to offer training services to a wider range of audiences. The targeted results of this effort included:

- Delivery of instructor led workshops developed from existing iSec curriculum.
- Identification, creation and customization of a distance learning system.

Online Learning Research and Development

An additional effort of the Cyber Training Center was the research and development of new online learning technologies and instructional design techniques that allowed for the effective and efficient delivery of timely and relevant training anywhere at any time. For example, iSec researchers explored areas ranging from new ways to deliver training to sailors on an aircraft carrier in the Mediterranean to researching new Human Computer Interfaces (HCI).

Another research aspect that was explored is the development of a primitive, but composable collection of metrics that measured the effectiveness of cyber security training programs and the technology used to identify and deliver content.

The targeted results for this research effort included:

– Analysis of instructional design techniques and new technologies that delivered content through new HCIs.

– Development of primitive metrics with discrete and quantitative properties that were applied to a pilot institution.

3.0 METHODS, ASSUMPTIONS AND PROCEDURES

This section presents the technical rationale, assumptions and procedures for the project tasks in security engineering, critical infrastructure protection, and cyber security training.

3.1 Security Engineering – Task 1

The research activities of the proposed effort were designed to improve the state of the art in security engineering technology, while complementing university computer science and information assurance curricula. Research results in the areas of security metrics and system security analysis, testing and validation have yielded new techniques and tools to help developers and engineers build high assurance information systems. Selected tools have been integrated into the curricular enhancements, exposing students to important concepts and practices in security engineering.

3.1.1 Technical Rationale and Assumptions.

The definition of security metrics embedded within practical tools for evaluating software, information system vulnerabilities and security countermeasures is fundamental to the field of security engineering. Scientists and engineers must be able to objectively measure artifacts and phenomena in their respective disciplines to understand systemic behavior and to exploit or cope with it. Unfortunately, security metrics for information technology are relatively shallow and incongruous, only considering surface-level exposures and not easily adaptable to different application

domains. The development of new security metrics that yield a context-sensitive view of vulnerability and exposure is a linchpin effort that impacts the educational activities and the other research activities in this project.

Distributed and embedded systems, such as those managing critical infrastructures, often have extreme performance and security requirements. Large enterprise information systems operate in their own kind of demanding environments. While the specific needs and requirements may differ, both classes of systems entail rigorous engineering methodologies to ensure their security. Moreover, vulnerabilities can reside at any level of a system, from bugs hiding in software to subtle errors in digital logic or mechanical behavior. Thus, any approach to fully validate the security properties of an information system must account for discrete and continuous behavior, along with potential interactions.

Compound exposure analysis offers an opportunity to understand the potential impact and likelihood of exploit for given vulnerabilities within an environmental and operational context. The core activity of compound exposure analysis is attack chaining, which iteratively evaluates vulnerabilities to determine if preconditions are satisfied for a given network state (step 1 of Fig. 1). If preconditions hold, an exposure is created for each vulnerability (step 2). Step 3 applies vulnerability postcondition functions to create a new network or system state (step 4). The process is repeated for each new state.

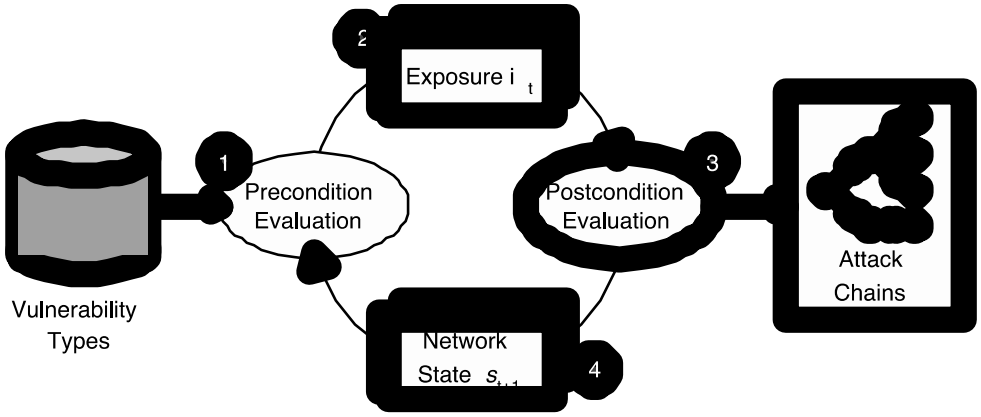

Figure 1. Compound exposure analysis

To date, compound exposure analysis and attack graphs primarily have been used in the domain of network security operations. However, the underlying idea is well-suited to supporting security engineering processes. In such an application, the compound exposure analysis at each layer is combined to yield a more comprehensive view of system vulnerability. In addition, this effort explored the development of a tool that encapsulates these measures and accordingly facilitates system security visualization.

Security engineering employs a range of techniques to generate confidence in the security properties of an information system. At one end of the spectrum, design and implementation review processes help analysts and programmers understand the consequences of decisions made in the system development process. At the other end, formal verification techniques offer the potential to guarantee the behavior of system components. In between, security testing and vulnerability scanning techniques help identify and eliminate flaws in systems. Each method plays a vital role in the security engineering process. The analytical techniques and tools developed from this project can be seamlessly integrated within an established security engineering methodology.

Ensuring the uptake and practice of security engineering methods mandates that they be captured and reflected in university computer science classes. Transforming university curricula to comprehensively integrate security engineering education is a formidable challenge. Instructors must create new instructional content and innovative educational experiences for students. They must change the way students are taught to program and design software solutions. Future information assurance professionals must be given a roadmap for applying security engineering processes and methodologies within their areas of specialization.

3.1.2 Methods and Procedures.

Primitive metrics relating likelihood and impact scores were developed to support the construction of more sophisticated measures that appreciate the context of system operation. Their composition under a common scheme permits the development of complex quantitative metrics that speak more directly to the core security properties of confidentiality, integrity and availability for a given information system.

At the software layer, quantitative measures for system vulnerability were investigated to leverage popular source code analysis tools [5, 6, 7, 8, 9]. The approach to bridge the gap between the hardware and software layers and to reveal latent system attack patterns relied on extending compound exposure analysis to incorporate system models and continuous behavior at the hardware level.

The approach adopted by this project has been to support the analytical framework and corresponding toolset development effort with a mathematical foundation capable of modeling the hybrid behavior of cyber physical systems. Identification of a suitable formalism with operational semantics creates an opportunity for both the designer and certifier to better understand the security properties of complex systems that drive critical infrastructures.

An additional benefit to embracing such a formalism as an analytical foundation is that it defines a pathway for system verification. A systematic translation of operational semantics into an axiomatic system permits verifiers to use special logics to prove specific model properties. Accordingly, the selection of an appropriate formalism has been shaped by the availability and capabilities of corresponding interactive theorem proving environments.

As the foundational formalism was identified, it has been welded into a compound exposure analysis framework. This entails the definition of a hybrid attack graph theory for generation and analysis. The resulting scheme permits the modeling and inspection of the attack space of cyber physical systems.

The hybrid attack graph theory is the basis for the development of tools to explore blended attack vectors that combine physical and cyber exploits. Tools developed incorporate features for cyber physical system specification, attack graph generation, and simple analysis. To support interaction, a rich interface and visualization substrate has been pursued.

Computer science and information technology courses equivalent to Introduction to Programming, Data Structures, Operating Systems, Database Systems, Computer Networks and Software Engineering (as titled and taught at the University of Tulsa) were identified by the curriculum enrichment efforts as targets for integration of secure software development instructional content. The curriculum development efforts are accompanied by exercises that expose students to practical tools and resources for security engineering processes.

Secure Programming

Tool construction in the discipline of secure programming is geared toward encouraging novice programmers to integrate analytical tools into their development process. A range of tools exist for static analysis on weakly typed languages such as C and Perl [21, 22, 23, 24], but student programmers do not embrace them. The efforts in this area have placed a premium on encouraging the adoption of practical tools with relatively simple analytical features, but high pedagogical value.

Information Assurance Courses

Curriculum development has occurred for existing information assurance course offerings. In Enterprise Security Management, students apply security engineering concepts and techniques to design, implement and protect an enterprise information network from the ground up. Modules that can be integrated within Information System Assurance embed metrics and methods of their application in the certification and accreditation phase of the course. Students in Network Security can use developed metrics and related analytical techniques to understand the consequences of competing network architectures and security solutions.

Information System Security Engineering

The curriculum development effort has profoundly influenced one class in particular, Information System Security Engineering (CS 5183). This class is offered on an annual basis and is designed to be a capstone course in the IA curriculum at the University of Tulsa (TU). In it, students validate the design and implementation of a secure system developed for a semester-long course project. The course emphasizes security engineering principles and processes in all phases of the System Development Life Cycle.

3.2 Critical Infrastructure Protection – Task 2

This initiative concentrated its efforts in establishing a state-of-the-art multipurpose laboratory for the protection of the critical infrastructure (CIPL) against cyber attacks in an academic setting.

3.2.1 Technical Rationale and Assumptions.

Process Control Systems (PCS) are widely used in electric power, manufacturing processes, chemical plant and refinery operations [25]. In a typical PCS implementation, sensors acquire data pertaining to process behavior; this data is then passed to control algorithms implemented in the PCS system. Depending on the sensor data and control objectives, output signals are sent to actuators that adjust controlled process to the desired state. In many industrial environments, sensors, actuators and control software are deployed in different locations, which requires the implementation of a communication infrastructure and the use of industrial protocols such as Modbus [26, 27, 28, 29] and DNP3 [30, 31, 32]. The use of Transmission Control Protocol / Internet Protocol (TCP/IP) as a carrier of industrial protocols has also allowed interconnections with corporate intranets and the Internet, exposing industrial systems to exploits and vulnerabilities that were not considered on the original design of these isolated systems. This task has focused on industrial protocols that have produced specs to carry control messages over TCP/IP. The implemented electric substation for instance is using DNP3, and more recently, as part of our no-cost extension efforts, this task has looked at an international effort lead by International Electrotechnical Commission (IEC) called IEC-61850. This new approach, popular in Europe and under evaluation in the US has been designed (from the ground up) to use Ethernet as the data-link layer of its network infrastructure.

It is important to recognize that while the Information Technology (IT) environment has already produced mature security solutions, they cannot be used directly in the PCS environment and new solutions will have to be specifically developed for this environment. We have designed components that interact well with the Critical Infrastructure by using the same industrial protocols found in the smart grid.

IT and PCS Environments

In developing effective solutions to secure the PCS networks used in the electric power sector, it was recognized that they differ from IT networks in several aspects. In terms of security principles, availability is the primary concern in PCS networks, followed by integrity and confidentiality while IT networks often emphasize confidentiality. PCS protocols, even those that employ a TCP/IP carrier, are not used in IT networks but the opposite does not apply; i.e., PCS networks are vulnerable to attacks originating from or targeting IT networks.

In addition, while many PCS protocols are based on open standards, vendors often augment protocols or use proprietary out-of-band mechanisms, such as web-based utilities for remote configuration, to provide additional functionality. In other words, unlike IT networks, protocol variations are quite common. There are also significant differences in terms of network traffic uniformity and volume. IT networks transport human-generated traffic that result in communication patterns that are difficult to predict. On the other hand, PCS network traffic is predictable. In terms of volume, traffic volume in PCS networks is very light compared to the massive amounts observed in IT networks. In fact, PCS protocol messages are quite short in length, e.g., Modbus messages never exceed 260 bytes when transported as the payload of a TCP packet.

3.2.2 Methods and Procedures.

This research thrust has addressed the significant need for PCS tools for critical infrastructure protection, and more specifically, for the electric power sector. We followed a systematic strategy to produce a comprehensive PCS security framework to mitigate risk in critical infrastructures. The resulting framework can be easily adapted to incorporate other protocols and its distributed nature should scale well.

The specific objectives (hardware and software) that were addressed were the following:

- Laboratory: Lab facilities designed not only to reflect, as accurately as possible, a typical electric power grid but also with the ability to incorporate and test new sensors and solutions.

- Cyber security Solutions: strategies for providing communication security to process control networks by using primitive technical controls.

- Training and Education: It is also important to note that training and education in CIP is important in helping to bridge the existing gap between IT security personnel and control engineers. To that effect a Critical Infrastructure Protection course was created at the graduate level. The course was open to Computer Science and Engineering students and it was designed to expose them to the challenges of process control networks, the history of critical infrastructure protection, regulations (mostly for the electric power sector) and programming

and use of embedded controllers. A second course on Mobile Application Development concentrated its efforts in the use of mobile platforms to develop HMIs (Human-Machine Interfaces)

Critical Infrastructure Laboratory

The laboratory was designed in accordance to a reference architecture that is representative of the main process control system components found in the electric power grid. In terms of functionality, a PCS system can be seen as a black box running control software and attached via inputs and outputs to the industrial process. Inputs of the control system, provided by sensors and transducers, are used to obtain state information of the industrial process. Control system outputs are mapped to switches and actuators to modify the state of the process as directed by the control software. Note that input, output and computing elements may not reside in the same location.

A PCS system, at an abstract level, consists of three major elements (Fig. 2): a control center, Remote Terminal Units (RTUs) and a communications infrastructure.

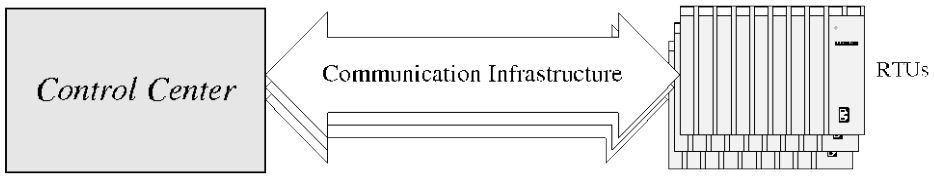

Figure 2. Fundamental components of process control systems

The following subsections describe the main three components designed and implemented throughout the laboratory: (i) electric power substation, (ii) Home Area network (HAN) facility and (iii) control room center.

Electric power substation

This laboratory houses a scaled-down electric power substation (Fig.3) that was used to validate our cyber-security framework for the Critical Infrastructure. The design of the substation closely reflects the topology of a ring-type substation with redundant lines as well as inductive and resistive loads. Input power levels are limited to voltage availability in the lab building. The substation uses three-phase 208V input voltage (dual inputs) and was designed for an estimated power consumption of 3KVA. The substation uses two controllers, also known as programmable logic controllers that communicate over an Ethernet network using the DNP3 protocol. This facility has all the elements needed to validate our approach on this cyber-physical system: physical (power input, switching relays), hardware interface (current and voltage transducers), software and control (programmable logic controllers) and communications (DNP3 over Ethernet).

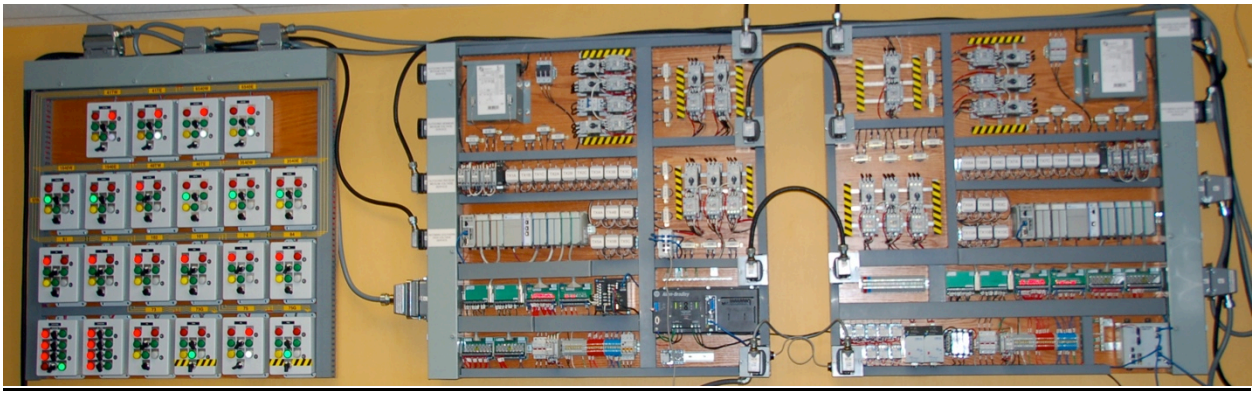

Figure 3. Scaled-down electric power substation

Control Room Center

The control room center is the central location where control and supervisory commands are issued. Human operators in the control center use Human Machine Interfaces (HMIs) that provide a convenient graphical environment to interact and supervise the system.

During the second half of the project, and after the electric power substation had been designed, we proceeded to design and implement a control center that would allow supervision and control of the smart grid. This included the design of suitable HMIs for the electric power substation. The prototype we built is centered on Rockwell-Automation solutions and uses a Jupiter server to drive two large screen displays. The Jupiter box is connected to the controllers using DNP3 over Ethernet. The Jupiter server is dual-homed. One interface is exposed to the control network using a private IP range and the other is exposed to the Internet to allow for remote access (Fig 4).

Figure 4. Control room center

Home Area Network (HAN)

The Home Area Network (HAN) includes a smart-meter and a home-automation setup that uses ZigBee. The goal was to implement, as accurately as possible, most of the planned features of the Smart Grid on the consumer side. We conducted a security analysis of the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard (ZigBee runs on top of IEEE 802.15.4) to help drive our security solutions. Using a toolkit called KillerBee (based on the Python scripting language) we implemented a monitoring systems capable of logging observed traffic. The data, viewable in Wireshark, can be extracted in a number of different formats, including plain text. In addition, we have incorporated the capability to store network data in a database. This will allow searching and development of query-based tools capable of producing relevant information based on a number of different characteristics such as transmitting device, timeline, frequency, etc. An outline describing our approach and architecture was accepted for inclusion as a chapter in the book “Securing Critical Infrastructures and Industrial Control Systems: Approaches for Threat Protection.

Situational Awareness and the Smart Grid

A framework to develop and cyber-security solutions was developed throughout the project. Our solution centered on the notion of situational awareness. Situational awareness is critical in any cyber-security solution. Inability to observe what happens in the control network effectively renders any solution blind. Packet filters and intrusion detection systems must be able to observe communication patterns and devices in the network. Our challenge was the development of a solution that was designed with industrial protocols in mind, which was distributed and scalable. A distributed monitoring solution, tested in our lab, was developed.

Our solution consists of four major components: (i) SCADA gateway, (ii) database, (iii) command center and (iv) network sensors (Fig. 5).

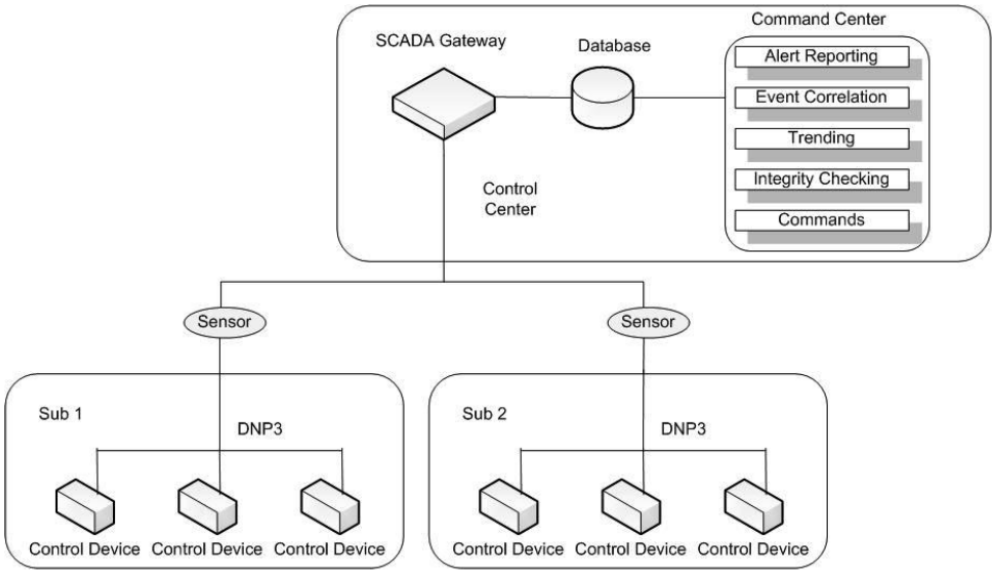

Figure 5. Distributed monitoring system

The network sensors operate in promiscuous mode to capture network traffic of interest. As a result, the sensors receive information about network topology, unit configuration, functionality and state of the devices, requested operations, function codes and other important pieces of information. The sensors timestamp the collected traffic, analyze it and forward relevant information to the SCADA gateway. In addition they may also help in locating attack signatures to identify malicious traffic. Therefore, these sensors can detect simple attacks where the intent is to interfere with the state of a single field device. Additionally, the sensors receive commands from the command center through the SCADA gateway. Upon receiving a specific command, a sensor may configure its network interface, start and stop scanning activities or generate a traffic analysis report.

The SCADA gateway collects the data gathered by sensors, translates them from different protocols into a canonical format and then forwards them to the database. Communication may also flow in the opposite direction to forward commands concerning configuration settings, scanning and generating reports from the command center to the sensors.

The database is the heart of the system. It provides a buffering interface between the SCADA gateway and the command center. The traffic stored in the database is used by the command center to provide state based traffic analysis. The database scheme includes information about system configuration, historical data, critical states, the network reference model and the network dynamic model.

Finally, the command center is a collection of applications that provide facilities for alert reporting, event correlation, integrity checking, trending and generating commands to be executed by the network sensors. State based traffic analysis is achieved by event correlation and prior knowledge of the critical system states. The command center verifies whether the system may enter into a critical state, as defined by the associated table in the database, and raises an alert. This approach will allow security practitioners to detect complex and coordinated attacks on industrial control system that may have a negative impact on overall availability and integrity. Time stamps are key elements in supporting the development of an accurate incident timeline from stored transactions. This will help operators in the command center to better recognize adversary intents, capabilities and trends, understand system vulnerabilities and identify new threats.

Work done under Task 2 has resulted in three M.S. Theses and eleven publications. Portions of this work were also included in a Patent Application for a compliance method for cyber-physical systems.

3.3 Cyber Security Training – Task 3

The training and research activities of this task were designed to improve the state of the art in cyber security training, while maintaining and updating university computer science and information assurance curricula.

The Cyber Security Training Center used and created new distance learning technologies and techniques to train government, military, law enforcement, and the private sector in digital forensics, information security, critical infrastructure protection, and cyber crime investigations. The center also sponsored seats in the facility for visiting military, government, law enforcement agents and private sector partners to provide hands-on training in laboratories while enabling them to interact with iSec researchers and student interns. Two visiting U.S. Army research scholars piloted this new capability in 2012.

The Cyber Security Training Center also focused on programs targeted across multiple audiences to raise awareness, drive interest and deliver niche training in the realm of information security. In particular, outreach programs where held to increase INFOSEC literacy and conscience of the community, in K-12 education (heightening interest as a

potential career path), and for small businesses. One arm of this effort created and delivered specialized technology training for government agencies and the private sector.

An additional branch of the Cyber Security Training Center focused on the research and development of new online learning technologies and instructional design techniques that allow for the effective and efficient delivery of timely and relevant training anywhere in the world. For example, iSec researchers explored areas ranging from new ways to deliver effective training to individual soldiers in other countries around the world to researching new collaborative Human Computer Interfaces (HCI) that were used for STEM education.

3.3.1 Technical Rationale and Assumptions.

The U.S. Department of Defense (DoD) established Directive 8570.1: Information Assurance Training, Certification and Workforce Management. This directive requires that all DoD Information Assurance technicians and managers are trained and certified to effectively defend DoD information, information systems and information infrastructures.

In today's environment of emerging security threats, the government has recognized the critical need for highly qualified, experienced information assurance personnel. To ensure a knowledgeable and skilled workforce the DoD has taken the necessary steps to develop requirements that involve the credentialing and continuing education of all DoD employees with privileged access to DoD information systems.

Specifically, the U.S. Department of Defense now requires every full- and part-time military service member, defense contractor, civilian and foreign employee with privileged access to a DoD system, regardless of job series or occupational specialty, to obtain a commercial certification credential that has been accredited by the American National Standards Institute (ANSI).

The Cyber Security Training Center currently offers instructor led and distance enabled security workshops centered on the Committee on National Security Systems (CNSS) 4011-4016 certifications and is scheduled to conduct multiple distance training courses with the U.S. Navy. In addition the Center also offers industry standard courses like the Certified Information Systems Security Professional (CISSP) certification that is accredited by the ANSI as well as additional cyber security continuing education opportunities for the government.

<u>Enterprise Security Training</u>

The need for useful and relevant cyber security training for the private sector has become more apparent and is a critical component of a successful security posture. For example, the University of Tulsa was recently approached by one of its industry partners requesting customized cyber security courses that could be delivered on-site.

In response, iSec developed continuing education courses in Best Practices in Secure Coding, Information Assurance and Security for Software Systems, Compliance and Legal Issues with IT Security and Privacy, Quality Assurance for Software Security, and Software Security Threat Modeling.

Critical Infrastructure Protection Training

As technology has become fully integrated into every aspect of the nation's critical infrastructure and, the security of these assets has become of paramount importance. Federal, state and local agencies, regulatory bodies and business organizations have all seen recent rules and regulations put in place that govern the levels of security compliance an entity must achieve. A key component of meeting these requirements is the training of the human resources within each organization in practical and current methodologies to ensure the security of these critical assets.

In 2006, the North American Electric Reliability Council implemented sweeping regulations that governed security of the critical infrastructure for the entire electrical power industry. A key component of these regulations is the training of human resources in the identification of risks and threats, and using best practices for securing assets and detection of compromised assets. Unfortunately, many organizations do not have a sufficient level of expertise in security to properly train their human resources. Indeed, several organizations do not have enough internal staff to deliver the training, even if the appropriate level of knowledge exists. The need for regular, relevant, and easy-to-use training ranging from security awareness to advanced SCADA security is essential for the protection of our nation's critical infrastructure assets.

Law Enforcement Training

Digital forensics and cyber crime investigations are rapidly changing fields, requiring law enforcement agencies to meet rigorous training requirements. New opportunities for committing criminal activity against individuals, organizations, or property are presented every day with the proliferation of personal digital devices, computer networks, automated data systems, and the Internet. Whether the crime involves attacks against computer systems, electronic information, or implicates digital devices in more traditional crimes such as murder, money laundering or fraud, electronic evidence is becoming more prevalent. It is no surprise that law enforcement and criminal justice officials are being overwhelmed by the volume of investigations and prosecutions that involve electronic evidence.

Fortunately, processes and procedures, as well as a variety of software and hardware tools have been developed to speed up and standardize the recovery of evidence from suspect media. Training on the proper use of these tools is crucial for recovering forensically sound evidence in a manner that will withstand legal scrutiny. In an attempt to remedy this lack of familiarity with digital evidence and to provide investigators with

an additional crime-fighting tool in their arsenal, training is made available by the National White Collar Crime Center. However, many smaller law enforcement agencies are unaware of this training or are unable to make use of it.

This has prompted iSec to development the Fundamentals of Cyber Crime Investigation and the Introduction to Digital Forensic Tools law enforcement Instructor Led workshops. These workshops were evaluated for conversion into online training modules that can be easily and quickly delivered to various personnel over a large geographic area in a format that allows them to work in conjunction with their schedules and capabilities. The success of future criminal investigations depends on the law enforcement community's access to timely, inexpensive, and readily available digital forensics and cyber crime investigations training material.

3.3.2 Methods and Procedures.

At the heart of the Cyber Security Training Center is iSec's dedication to the curriculum design, development and conversion of our high-end security curricula. iSec utilized its security faculty and external Subject Matter Experts (SME) to identify existing iSec security courses and curriculum that were converted into continuing education offerings and has developed new training courses for the public and private sectors. Throughout this process instructional design specialist evaluated the learning style that is the most appropriate for each offering. It is important to note that not all security courses and curriculum is suited for online training. In this case instructor led courses or workshops were developed and delivered through the University of Tulsa's Continuing Engineering and Science Education department. Finally, internal and external online curriculum development specialists were used to create the high end, immersive training environments.

The Cyber Security Training Center also used a variety of content delivery methodologies beginning with instructor led workshops and evolving into a robust distance training system. While instructor led workshops are an important aspect of continuing education, the identification and conversion of appropriate security content into an effective online format is critical. With the use of topic level modules and role-based training techniques, the Cyber Security Training Center is positioned to offer cyber security training opportunities to a wider audience in the future.

An additional branch of the Cyber Security Training Center is the research and development of new online learning technologies and instructional design techniques that allow for the effective and efficient delivery of timely and relevant training anywhere at any time. Following are areas the Cyber Security Training Center focused on through this life of the project.

– E-Learning Technologies: Throughout the course of this project, new e-learning technologies were evaluated and gaps become apparent. The Cyber Security Training Center worked towards advancing the state-of-the-art in e-learning by not only identifying these gap, but creating solutions that will help fill them. The Cyber Security Training Center also worked towards creating next generation

online training environments that blend instructor led, e-learning, distance learning, and even mobile computing technologies and techniques.

– Human Computer Interaction: The Cyber Security Training Center developed a robust research program and curriculum in Human Computer Interaction (HCI) centered around innovative, unobtrusive, and intuitive user interfaces for traditional desktop computers, small handheld devices and large-scale multi-user systems. These interfaces enabled and encouraged collaboration between users, and strived to produce interfaces that allowed the user to focus on interacting with the information being presented rather than how to interact with the information. Studies performed during this project have shown that these collaborative interfaces have many promising applications in group learning and training.

– Cyber Security Training Evaluation Metrics: An additional research aspect explored throughout this project is the development of a primitive, but composable collection of metrics to measure the effectiveness of cyber security training programs and the technology used to identify and deliver the training content. A study was performed on the impact of instructor led versus online training for retention, as well as on the effectiveness of the instructional design methodologies used to create the training content and the technology used to deliver it.

4.0 RESULTS AND DISCUSSION

This section presents the results for the project efforts in security engineering, critical infrastructure protection, and cyber security training.

4.1 Security Engineering – Task 1

Research, education and outreach initiatives of the security engineering group built on existing competencies in formal methods, engineering methodology and pedagogies to yield tangible results and accomplishments that translate to the field. The driving themes that profoundly influenced the direction of the work were: cyber physical systems, practical analytics and “big data.”

Research initiatives in the tools and metrics groups pursued overlapping lines of inquiry in the construction and evaluation of security analysis tools. Foundational work was performed to understand blended attack vectors spanning cyber and physical domains. This yielded the Hybrid Attack Graph (HAG) and a web-based HAG generation tool called RAVEN:Wing. A composite metric based on likelihood and impact measures was developed for attack graphs to support deeper insights into the risk associated with multi-stage attacks.

A network security analysis tool chain composed of open source software was

developed and evaluated as part of an applied research and outreach effort in collaboration with a major oil and gas company headquartered in Tulsa, Oklahoma. The tool chain and accompanying methodology confronts serious challenges posed by large heterogeneous networks (e.g., SCADA and corporate systems) from which massive volumes of security data are collected.

Curriculum development and enrichment focused energies on the construction of new modules for integration within graduate-level university courses in information assurance and within specialty short courses offered to industry. In addition to a suite of lectures, labs and exercises covering topics such as security engineering

methodologies, information assurance principles, security audit and analytics, a special track in secure coding was developed and deployed both in short course form and in a graduate level offering at The University of Tulsa.

In terms of scholarly output, the Security Engineering group has produced 23 publications - - 16 articles (defined as peer-reviewed conference or journal papers and abstracts), five MS theses, 1 technical report and 1 patent application. Six graduate students supported by the Defense Advanced Research Projects Agency (DARPA) project have completed their Masters degrees and four are pursuing PhD degrees in Computer Science.

4.2 Critical Infrastructure Protection – Task 2

In line with the stated objectives, a laboratory was designed and built to support research and educational activities. The laboratory is representative of major components found in the power grid and its components are fully networked to support development of cyber-security tools appropriate for this delicate domain. In addition to the tools and accomplishments listed below, a simulation framework was designed to study and analyze cyber-physical systems. The electric grid is a good example of a cyber-physical system and this type of tools, that bring together analog and discrete components, can be extended for use in other domain such as in process control systems (also known as SCADA systems).

The Critical Infrastructure Lab at the University of Tulsa designed and constructed a scaled-down power substation. Power substations, which are an important component of Smart Grids, contain a number of critical assets such as transformers, circuit breakers, PLCs and safety devices. The PLCs used to control the function of the substation communicate over DNP3 TCP/IP. The substation follows a ring-type design with redundant lines. There are two three-phase inputs at 240 Voltage Alternating Current (VAC) that are subsequently transformed to 208 VAC (three phase), that means 120 VAC (one phase) for the end consumer. A control room center was also designed to visualize and understand the type of protocols and equipment used by system operators.

A Situational Awareness (SA) framework was designed to provide support for cyber-

security tools. The framework required the use of network sensors deployed at strategic points in the control network and were linked back to a SCADA gateway. The gateway then communicates with a database and the control center to provide SCADA operators with a better understanding of the entire system. This large-scale data collection system would ideally provide a complete view of the components, behavior, and performance of SCADA devices and enable further intelligent analysis of their communications in order to anticipate problems before disruptions arise.

To further support our goals, a Modular Framework For Auditing SCADA Applications (MoFASA) was also developed. The framework uses fuzzing as the testing mechanism for the embedded devices (such as PLCs) that form the core of most critical networks. This framework is intended for use by end-users who, while technically savvy, may not have experience in security research or vulnerability testing. It is hoped that this framework will assist device manufacturers and facility operators in assessing and improving the security of their devices. It will also serve as an important research tool.

On the user side of the Smart Grid, there are also security issues associated with the use of smart meters that communicate with home automation devices (such as a thermostat or a switch) using a wireless protocol called ZigBee. Information transmitted over this network also needs protection. A distributed monitoring system for ZigBee wireless networks was implemented and also tested in the CIP laboratory.

Efforts in the area of simulation of smart grid components and protocols have resulted in the implementation of a simulation framework for cyber-physical systems. This effort was built on top of a discrete-even simulator called OMNET++ that offers good modularity as well as strong support for messaging. Even though OMNET++ is a discrete event simulator, physical systems can be simulated by using the notion of self-messages (to simulate passage of time) and common numerical integration techniques.

Two courses were created and taught as a result of work done in Task 2. The first course, “Critical Infrastructure Protection,’’ was a graduate level course offered to CS and Engineering students to instruct them on the history and challenges associated with protecting critical infrastructure. The course also had a lab component were students learned how to program and network the PLCs (programmable logic controllers) that are typically used to control these systems. The second course, “Mobile Application Development’’, concentrated efforts in the implementation of HMIs (Human Machine Interfaces) using mobile devices and touch screens.

Scholarly activity by the Task 2 group has produced 11 peer-reviewed papers, three MS theses and one patent application. Four graduate students supported by this DARPA project completed their Master degrees and two are pursuing PhD degrees.

4.3 Cyber Security Training – Task 3

The Cyber Security Training Center created and delivered multiple workshops over the life of the grant. This includes the design, development and delivery of a suite of five cyber security evening and distance enabled classes that are mapped to the CNSS 4011-4012 federal certifications and grant 15 hours of college credit; delivery of one-day security workshops targeted to information security auditors that included topics in: Internet security, information security policy development, information privacy, social networking safety, mobile device security, and trends in digital commerce; delivery of multiple three-day secure coding workshops; design and development of a new digital forensics workshop; and the creation of various cyber security modules and short courses.

The Cyber Security Training Center's content development team also performed community outreach that included free to the public cyber security workshops, as well as elementary school Science Technology Engineering and Mathematics (STEM) education program support (Fig. 6). Team members designed a collaborative STEM education game centered on mathematics. Using a multi-touch table to deliver the content, elementary school students worked through traditional math problems in groups of four where no one student could solve the problem. This resulting in students interactive socially, to think critically and ultimately solve math problems logically.

Figure 6. Collaborative STEM education multi-touch devices

The Cyber Security Training Center's content delivery team completed the design and construction of a distance learning enabled Cyber Security Applied Classroom. This applied classroom includes video conferencing capabilities, a bridge that enables 20 multi-point connections, live and archived streaming encoding and delivery, content organization/sharing, and a mobile videoconferencing cart to be used throughout iSec's research facility to broadcast applied laboratory assignments that utilize the unique equipment in each of iSec's research laboratories. This applied classroom was used to

deliver multiple workshops over the last three years and will be extensively used to deliver cyber security training to our government and private sector partners after the life of the grant.

The Cyber Security Training Center's research and development team completed construction of the Collaborative Analytical Visualization Environment (CAVE) multi-touch research platform and the spatially aware Human Computer Interface (HCI) research laboratory (Fig. 7). Through the HCI laboratory, the research and development team also completed research that generated working prototypes in spatial access control, gesture oriented data sharing, mobile redaction bubbles and new multi-user collaborative interfaces. In addition, the research and development team completed phase one work with our psychology partners on the evaluation and creation of a security metrics model to assess the security posture of an organization and explore how cyber security training can influence that posture. The team completed the integration of live and historic filtered data from TU's network into the model based on recent permission from TU's IT department. A white paper on the phase one results was generated and work will continue through phase two efforts after the end of the grant period.

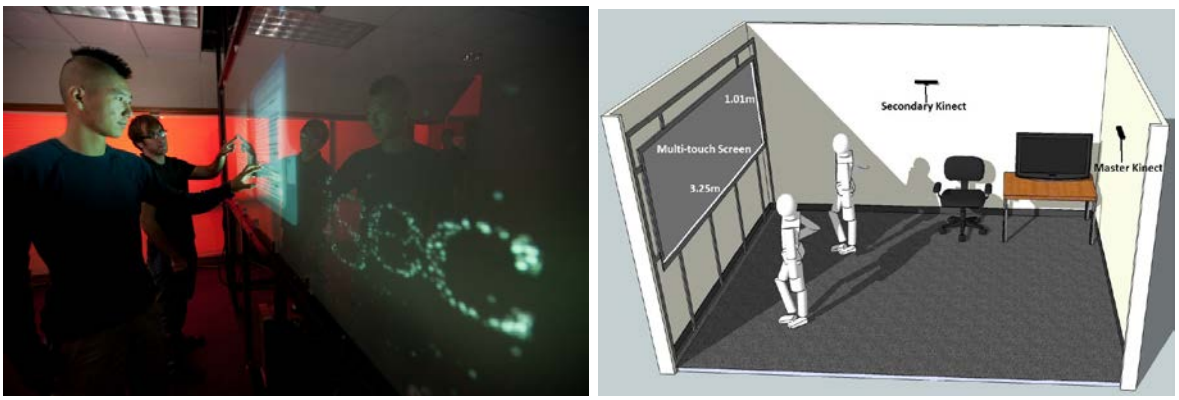

Figure 7. Human Computer Interaction Laboratory

In terms of scholarly output, the Cyber Security Training group has produced eight publications, two MS theses, and one technical report. Three graduate students supported by the DARPA project have completed their Masters degrees and two are pursuing PhD degrees in Computer Science.

5.0 CONCLUSION

The Security Engineering and Educational Initiatives for Critical Information Infrastructures project has enabled the Institute for Information Security to significantly enhance its research infrastructure, as well as discover new multi-disciplinary research lines previously unexplored. The project has supported thirteen MS and eight PhD graduate student researchers. It has also produced 40 publications and one patent application over the 3-year project. The list below highlights the project accomplishments and deliverables broken out by task.

Project Accomplishments

Security Engineering - Task 1

- Security analytics tool chain and methodology for SCADA systems
- Hybrid attack graph formalism and tool (HAG and RAVEN:Wing)
- Security engineering curriculum (modules, labs and exercises for security audit, analytics and secure coding)

Critical Infrastructure Protection - Task 2

- Design and construction of scaled-down electric power substation using redundant networked controllers
- Home Area Network (HAN) setup to interface with smart meters using ZigBee
- Situational awareness tools for electric power substation and HANs
- Intelligent testing framework for embedded devices (MoFASA)
- Simulation framework for cyber-physical systems (using OMNET++)
- Design and construction of a control room network
- Curriculum development

Cyber Security Training - Task 3

- Completion of the Cyber Security Applied Classroom

- Creation and delivery of multiple cyber security workshops and courses
- Completed construction of the Collaborative Analytical Visualization Environment (CAVE) research platform
- Completed phase one study of security metrics model
- Performed community outreach that included public cyber security workshops and elementary school STEM education program support

Project Deliverables

Security Engineering - Task 1

A. Security analytics tool chain, methodology and hardware architecture
B. RAVEN multi-touch prototype
C. RAVEN:WING web interface to hybrid attack graph generator prototype, v1.1
D. Three Attack scenarios (Conficker, Substation, and Automotive)
E. “Secure Coding“ Instructional Module: Slides and project
F. ISSEP exercise and instructional modules: Slides and project
G. “The New Age of Cyber (In)Security“ Instructional Module: Slides
H. “Threat Modeling“ Instructional Modules: Slides and Labs
I. “Applied Cryptography” Instructional Modules: Slides and Labs
J. “Security Analytics“ Instructional Modules: Slides and Labs
K. Cyber Security for Electric Cooperatives instruction modules.
L. Security Audit curriculum (13 modules).
M. Secure Coding curriculum (10 modules).

Critical Infrastructure Protection - Task 2

A. Control room center for the electric power sector
B. Home Area Network set-up with ZigBee and Smart Meters

C. Cyber-physical system simulation framework

D. Home Area Networks monitoring systems

E. Situational awareness tools for the smart grid

F. Testing framework for embedded devices using fuzzing (MoFASA)

G. Critical Infrastructure Protection course (full semester, 3 credit-hour)

H. Various papers and theses

Cyber Security Training - Task 3

A. Fully functional online learning enabled cyber security applied classroom

B. Suite of five cyber security evening and distance enabled classes that are mapped to the CNSS 4011-4012 federal certifications and grant 15 hours of college credit

C. Three-day Secure Coding workshop

D. One-day Information Security workshop

E. Three-day Digital Forensics workshop

F. Various cyber security short courses

G. Security Metrics study and white paper

H. Collaborative user interface prototypes

I. Spatial access control prototype

J. Gesture oriented data sharing prototype

K. Mobile redaction bubble prototype

L. Various papers and theses

6.0 REFERENCES

[1] Saltzer J. and Schroeder M., "The protection of information in computer systems", *Proceedings of the IEEE*, **63**(9):1278–1308, 1975.

[2] Dawkins J., *A systematic approach to multi-stage network attack analysis*, Master's thesis, University of Tulsa, 2003.

[3] Dawkins J., Campbell C., Larson R., Fitch K., and Tidwell T., "Modeling network attacks: Extending the attack tree paradigm", *Proceedings of the Third Annual International Systems Security Engineering Association Conference*, 2002.

[4] Tidwell T., Larson R., Fitch K., and Hale J., "Modeling internet attacks," *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, June 2001.

[5] Cigital, "ITS4: Software security tool", http://www.cigital.com/its4/. Accessed June 4, 2012.

[6] Ounce Labs. "Prexis". http://www.ouncelabs.com/, IBM Security AppScan Source. Accessed June 4, 2013.

[7] Secure Software, "Codeassure". http://www.securesoftware.com/.

[8] Splint. Splint: Annotation-assisted lightweight static checking. http://www.splint.org/. Accessed June 4, 2013.

[9] Wheeler D., Flawfinder. http://www.dwheeler.com/flawfinder/. Accessed June 4, 2013.

[10] Office of the Press Secretary, *Critical Infrastructure Identification, Prioritization, and Protection*, Technical Report HSPD7, Executive Office of the President, Washington, DC, 17 December 2003.

[11] Kannberg L., Chassin D., DeSteese J., Hauser S., Kintner-Meyer M., Pratt R., Schienbein L., and Warwick W., *Gridwise: The benefits of a transformed energy system*, Technical Report 14396, Pacific Northwest National Laboratory, 2003.

[12] Instrumentation Systems and Automation (ISA) Society, *Integrating Electronic Security into the Manufacturing and Control Systems Environment*, Technical Report ANSI/ISA- TR99.00.02-2004, American National Standards Institute (ANSI), 2004.

[13] Instrumentation Systems and Automation (ISA) Society, *Security Technologies for Manufacturing and Control Systems*, Technical Report ANSI/ISA-TR99.00.01-2004, American National Standards Institute (ANSI), 2004.

[14] American Petroleum Institute, *SCADA Security*, Technical Report API 1164, American Petroleum Institute, 2004.

[15] American Gas Association, *Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan*, Technical Report AGA Report No. 12 (Part 1), 2005.

[16] American Gas Association, *Cryptographic Protection of SCADA Communications; Part 2: Retrofit Link Encryption for Asynchronous Serial Communications*, Technical Report AGA Report No. 12 (Part 2), 2005.

[17] British Columbia Institute of Technology (BCIT), *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, Technical report, National Infrastructure Security Coordination Centre (NISCC), London, United Kingdom, 2005.

[18] Decisive Analytics, "System Protection Profile - Industrial Control Systems", *System Protection Profile SPP-ICS, NIST*, 2004.

[19] Falco J., Stouffer K., and Kent K., *Guide to supervisory control and data acquisition (SCADA) and industrial control systems security*, NIST Special Publication 800-82, NIST, 2006.

[20] Energetics Incorporated, "Roadmap to Secure Control Systems in the Energy Sector", *Roadmap eRoadmap*, US Department of Energy, 2006.

[21] Chen H. and Wagner D., "MOPS: an infrastructure for examining security properties of software", *Proceedings of the 9th ACM conference on Computer and communications Security*, pp. 235–244, ACM Press, 2002.

[22] Cowan C., "Software security for open-source systems", *IEEE Security and Privacy*, 1(1):38–45, 2003.

[23] Kohno Y., Veiga J., Bloch J. T. and McGraw G., "ITS4: A static vulnerability scanner for C and C++ code", *Proceedings of the Annual Computer Security Applications Conference*, Chapman & Hall, Ltd., 2000.

[24] Wagner D., *Static analysis and computer security: new techniques for software assurance*, Ph.D. Dissertation, University of California at Berkeley, 2000.

[25] Boyer S. A., SCADA: Supervisory Control and Data Acquisition, ISA - Instrumentation, Systems, and Automation Society, 3rd Edition, 2004.

[26] Modbus IDA, *MODBUS Application Protocol Specification*, Modbus IDA, 6 April 2004.

[27] Modbus IDA, *MODBUS Messaging on TCP/IP Implementation Guide*, Modbus IDA, 4 June 2004.

[28] Modbus.org, *MODBUS Over Serial Line Specification - Implementation Guide*, modbus.org, February 2002

[29] Inc. Modicon, *MODBUS Protocol Reference Guide*, Modicon, Inc., June 1996.

[30] Smith M. and Copps M., *DNP3 V3.00 Data Object Library Version 0.02*, Technical report, DNP Users Group, 1 September 1993.

[31] Smith M. and McFadyen J., *DNP V3.00 Data Link Layer Protocol Description*, Technical report, DNP Users Group, June 2000.

[32] Thesing M., *Transporting DNP V3.00 over Local and Wide Area Networks*, Technical report, DNP Users Group, December 1993.

APPPENDIX A

List of publications over the 3 year project (40 total publications)

Patent Application Combining SE and CIP Groups (in preparation)

Hawrylak, P., Papa, M., and Hale, J., *Compliance Method for a Cyber-Physical System*, Institute for Information Security, The University of Tulsa, Tulsa, OK, January 2013.

Security Engineering – Task 1

Butler, M., Reed S., Hawrylak P., and Hale J., "Implementing Graceful RFID Privilege Reduction (Extended Abstract and Poster)," *Extended Abstract 8th Annual Cyber Security and Information Intelligence Research Workshop,* Oak Ridge, TN January 7-9, 2013.

Staggs J., Fisher M., Hale J., and Haney M., *Incident Discovery on Enterprise Networks Using Passive Monitoring Techniques,* Technical Report, Institute for Information Security, The University of Tulsa, Tulsa, OK, January 2013.

Hartney, C., *Security Risk Metrics: An Attack Graph-Centric Approach,* MS Thesis, The University of Tulsa, July 20, 2012.

Hawrylak, P., Hale J. and Papa, M., "Security Issues for ISO 18000-6 Type C RFID: Identification and Solutions," i*n Developments in Wireless Network Prototyping, Design and Deployment: Future Generations*, M. A. Matin, Ed., IGI Global, pp. 38-55, Hershey, PA, May, 2012, (ISBN-13: 978-1-4666-1797-1)

Link: http://www.igi-global.com/chapter/security-issues-iso-18000-type/67004

Hawrylak, P., Haney, M., Hale J. and Papa, M., "Using Hybrid Attack Graphs to Model Cyber Physical Attacks in the Smart Grid," *in Proceedings of the 5th International Symposium on Resilient Control Systems*, Salt Lake City, Utah, August 14-16, 2012.

Link:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6309311&isnumber=6309281

Hawrylak, P., Hale J. and Papa, M., "Using Hybrid Attack Graphs to Model and Analyze Attacks Against the Critical Information Infrastructure*," in Critical Information Infrastructure Protection and Resilience in the ICT Sector,* eds. Theron and Bologna, IGI Global, Hershey, PA, (2012).

Link: http://www.igi-global.com/book/critical-information-infrastructure-protection-resilience/70773

Hawrylak, P., Schimke, N., Hale J. and Papa, M., "RFID in E-Health: Technology, Implementation, and Security Issues," *in Telemedicine and E-Health Services, Policies and Applications: Advancements and Developments*, eds. Rodrigues, Diez and Sainz de Abajo, IGI Global, Hershey, PA, pp. 347-368, (2012).

Link: http://www.igi-global.com/chapter/rfid-health-technology-implementation-security/64994

Louthan, G., *Hybrid Attack Graphs for Modeling Cyber Physical Systems*, M.S. Thesis, The University of Tulsa, Tulsa, OK, November 17, 2011.

Louthan, G., Hardwicke, P., Hawrylak, P., and Hale J., "Toward Hybrid Attack Dependency Graphs," *Extended Abstract in 7th Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, TN, Oct 12-14, 2011.

Link: http://dl.acm.org/citation.cfm?id=2179368

Butler, M., Hawrylak, P., and Hale J., "Graceful Privilege Reduction in RFID Security," *Extended Abstract in 7th Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, TN, Oct 12-14, 2011.

Link: http://dl.acm.org/citation.cfm?id=2179298.2179349&coll=DL&dl=GUIDE&CFID=258109095&CFTOKEN=32012928

Hartney, C., Louthan, G. and Hale J., "Risk Metric for Attack Dependency Graphs," *Extended Abstract in 7th Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, TN, Oct 12-14, 2011.

Butler, M., *Dynamic Risk Assessment Access Control*, MS Thesis, The University of Tulsa, March 24, 2011.

Roberts, A., *Mitigating Automated Patch-Based Exploit Generation with Encrypted Update Distribution*, MS Thesis, The University of Tulsa, November 5, 2010.

Singleton, E. et al., "RAVEN: Real-time Attack Visualization through Examining Network Flows", *2010 Annual Computer Security Applications Conference*, Austin, TX, December 9, 2010.

Link: http://www.acsac.org/2010/program/posters/singleton.pdf

Gehres P., Singleton N., Louthan G., and Hale J., "Toward Sensitive Information Redaction in a Collaborative, Multilevel Security Environment," in *6th International Symposium on Wikis and Open Collaboration (WikiSym 2010)*, July 7 - 9, 2010.

Link: http://dl.acm.org/citation.cfm?id=1832793

Louthan, G., Roberts, A., Butler, M., and Hale J., "The Blunderdome: An Offensive Exercise for Building Network, Systems, and Web Security Awareness," in *USENIX*

Workshop on Cyber Security Experimentation and Test (CSET '10), Washington DC, August 9, 2010.

Link: http://dl.acm.org/citation.cfm?id=1924556

Roberts, A., Johnson, C., and Hale J., "Transparent Emergency Data Destruction," *Air Force Institute of Technology (AFIT)*, Wright Patterson AFB, Dayton, Ohio, April 8-9, 2010.

Link: http://academic-conferences.org/iciw/iciw2011/iciw10-proceedings.htm

Critical Infrastructure Protection – Task 2

Hawrylak, P., Nivethan, J., and Papa, M., "Automating Electric Substations using IEC 61850," *in Systems and Optimization Aspects of Smart Grid Challenges*, P.M. Pardalos, M. Carvalho and V. Pappu (Eds.), Springer, (2012).

Brundage, M., Mavridou, A., Johnson, J., Hawrylak, P., and Papa, M., "Distributed Monitoring: A Framework for Securing Data Acquisition," Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection, C. Laing, A. Badii and P. Vickers (Eds.), DOI:10.4018/978-1-4666-2659-1.ch006, IGI Global, pp. 144–167, Hershey, PA, (2012).

Link: http://www.igi-global.com/chapter/distributed-monitoring-framework-securing-data/73123

Mavridou, A., Zhou, V., Dawkins, J., and Papa, M., "A Situational Awareness Framework for Securing the Smart Grid using Monitoring Sensors and Threat Models," in *International Journal of Electronic Security and Digital Forensics - Special Issue on Global Security, Safety and Sustainability*, Vol. 4, Nos. 2/3, pp. 138–153, (2012).

Link: http://www.inderscience.com/info/inarticle.php?artid=48417

Schimke, N., Hale J., Papa, M., and Hawrylak, P., "Security Risks Associated with Radio Frequency Identification in Medical Environments," in *Journal of Medical Information Systems, (2012).*

Link: http://link.springer.com/article/10.1007%2Fs10916-011-9792-0

Hawrylak, P., Hale J. and Papa, M., Security Issues for ISO 18000-6 Type C RFID: Identification and Solutions," Developments in Wireless Network Prototyping, Design and Deployment: Future Generations, ISBN 978-1-4666-1799-5, M. A. Matin Ed., IGI Global, pp. 38–55, (2012).

Link: http://www.igi-global.com/chapter/security-issues-iso-18000-type/67004

Schimke, N., Hale J., Papa, M., and Hawrylak, P., "Security Risks Associated with Radio Frequency Identification in Medical Environments," in *Journal of Medical Systems Special Issue on Radio Frequency Identification in the Healthcare Sector: Applications, Business Models, Drivers and Challenges*, Springer, Vol. 36, No. 6, pp. 3491–3505, (2012).

Link: http://link.springer.com/article/10.1007%2Fs10916-011-9792-0

Nivethan, J., Papa, M., and Hawrylak, P., "Estimating link availability and timing delays in Ethernet-based Networks," in *Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop*, October 30-November 1, Oak Ridge, Tennessee, (2012).

Hawrylak, P., Louthan, G., Daily, J., Hale, J., and Papa, M., "Attack Graphs and Scenario Driven Wireless Computer Network Defense," Situational Awareness in Computer Network Defense: Principles, Methods and Applications, Cyril Onwubiko and Thomas Owens (Eds.), ISBN 978- 1-4666-0104-8, IGI Global, Hershey, PA, pp. 284–301, (2011).

Link: http://www.igi-global.com/chapter/attack-graphs-scenario-driven-wireless/62387

Mavridou, A., and Papa, M., "A Situational Awareness Architecture for the Smart Grid," in *Proceedings of the Seventh International Conference in Global Security Safety and Sustainability* (held jointly with the Fourth International Conference on e- Democracy, Thessaloniki, Greece, August 24–26,pp. 229–236, (2011).

Link: http://link.springer.com/chapter/10.1007/978-3-642-33448-1_31

Mavridou, A., *A Situational Awareness Framework for the Smart Grid,* M.S. in Computer Science, University of Tulsa, Tulsa, OK, April 30, 2012.

Brundage, M., *Distributed Monitoring System for ZigBee Wireless Networks,* M.S. in Computer Science, University of Tulsa, Tulsa, OK, April 9, 2012.

Johnson, J., *MoFASA: A modular framework for auditing SCADA applications,* M.S. in Computer Science, University of Tulsa, Tulsa, OK, November 14, 2011.

Cyber Security Training – Task 3

Jackson A., Brummel, B., Pollet, C., and Greer, D., "An Evaluation of a Face-to-Face Collaborative Technology in Elementary Math Education," in *Education Technology Research and Development Journal,* January 2013.

Harbort, Z., and Fellin, C., "Gesture-Oriented Data Sharing," in *8th Annual Cyber Security and Information Intelligence Research*, January 8-10, 2013.

Harbort, Z., *A Device Fusion Framework for Secure Collaborative Environments,* M.S. in Computer Science, University of Tulsa, Tulsa, OK, December 2012.

Harbort, Z., Greer, D., "Identity Issues in Collaborative Natural User Interface Environments," in *ID360 Proceedings,* Austin, TX, April 2012.

Jackson A., Brummel, B., Pollet, C., Kong, L., and Greer, D., "Facilitating Math Growth Using Collaborative Multi-User Multi-Touch Technology," in *Eighty-sixth Regional Meeting of the American Association for the Advancement of Science Southwestern and Rocky Mountain Division,* April 2012.

Kong, L., Hale, J. and Greer, D., "Spatial Identity Awareness for Collaborative Environments," in *Proceedings of International Symposium on Security in Collaboration Technologies and Systems*, Denver, Colorado, May 21, 2012.

Link:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6261093&isnumber=6261004

Kong, L., *Spatial Access Control on Multi Touch User Interface*, M.S. in Computer Science, University of Tulsa, Tulsa, OK, November 30, 2011.

Harbort Z., Louthan, G., and Hale, J., "Techniques for Attack Graph Visualization and Interaction," Extended Abstract in *7th Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, TN, Oct 12-14, 2011.

Link:http://dl.acm.org/citation.cfm?id=2179298.2179383&coll=DL&dl=ACM&CFID=258109095&CFTOKEN=32012928

Gehres, P., Louthan, G., Roberts, W., and Hale, J., "Evaluating a Higher Education Information Assurance Program with the Collegiate Cyber Defense Competition," in *3rd Workshop on Cyber Security Experimentation and Test*, Washington DC, August 9, 2010.

Pollet, C., and Hale, J., "Collaborative User Interfaces," in *AISES National Conference,* October 30, 2009.

LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

American Gas Association (AGA)

American National Standards Institute (ANSI)

Certified Information Systems Security Professional (CISSP)

Collaborative Analytical Visualization Environment (CAVE)

Committee on National Security Systems (CNSS)

Computer Science (CS)

Critical Infrastructure Protection (CIP)

Critical Infrastructure Protection Laboratory (CIPL)

Defense Advanced Research Projects Agency (DARPA)

Department of Defense (DoD)

Department of Energy (DOE)

Distributed Network Protocol (DNP3)

Doctor of Philosophy (PhD)

Home Area network (HAN)

Homeland Security Presidential Directive (HSPD)

Human Computer Interaction (HCI)

Human Machine Interfaces (HMIs)

Hybrid Attack Graph (HAG)

Information Assurance (IA)

Information Technology (IT)

Institute for Information Security (iSec)

Institute of Electrical and Electronics Engineers (IEEE)

Instrumentation Systems and Automation (ISA)

International Electrotechnical Commission (IEC)

Master of Science (MS)

Modular Framework For Auditing SCADA Applications (MoFASA)

National Infrastructure Security Co-ordination Centre (NISCC)

National Institute for Standards and Technology (NIST)

Presidential Decision Directive 63 (PDD63)

Process Control Systems (PCS)

Programmable Logic Controllers (PLCs)

Public Key Infrastructure (PKI)

Remote Terminal Units (RTUs)

Science Technology Engineering and Mathematics (STEM)

Situational Awareness (SA)

Subject Matter Experts (SME)

Supervisory Control and Data Acquisition (SCADA)

Transmission Control Protocol / Internet Protocol (TCP/IP)

United States (U.S.)

University of Tulsa (TU)

Voltage Alternating Current (VAC)